UNITED STATES DISTRICT COURT
DISTRICT OF MINNESOTA

SANDRA GROOM, individually and on behalf of all others similarly situated, Plaintiff, v. UNITEDHEALTH GROUP INCORPORATED; UNITEDHEALTHCARE, INC.; OPTUM, INC.; and CHANGE HEALTHCARE INC., Defendants.	Case No. 24-cv-00915 **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiff Sandra Groom ("Plaintiff") initiates this Class Action Complaint against Defendants UnitedHealth Group Incorporated, UnitedHealthcare, Inc., Optum, Inc., and Change Healthcare Inc. (collectively, the "Defendants" or "UHG") in her individual capacity and on behalf of others similarly situated. Plaintiff asserts the following allegations based on her personal knowledge of her own actions, as well as investigations conducted by her counsel, and upon information and belief regarding all other relevant matters:

NATURE OF ACTION

1. UnitedHealth Group Incorporated, a massive healthcare conglomerate, includes UnitedHealthcare, Inc. and three Optum, Inc. divisions: Optum Health, OptumInsight, and Optum Rx (collectively, "Optum").[1]

[1] *UnitedHealth Group Incorporated (UNH)*, FORBES, https://www.forbes.com/companies/unitedhealth-group/?sh=ee01a2f7cb0d (last visited Mar. 11, 2024).

2. Change Healthcare, Inc. ("Change Healthcare") is among the largest prescription medication processors in the United States, managing billing for over 67,000 pharmacies nationwide and facilitating 15-billion healthcare transactions annually.[2]

3. In October 2022, UnitedHealth Group Incorporated finalized its acquisition of Change Healthcare and integrated it with OptumInsight "to provide software and data analytics, technology-enabled services and research, advisory and revenue cycle management offerings to help make health care work better for everyone."[3]

4. In or around February 2024, UHG experienced one of the most significant data breaches in U.S. history. A ransomware group claims to have breached UHG's servers and obtained 6 terabytes of crucial confidential and highly sensitive data. This breach has led to network disruptions that have already affected millions of patients and healthcare providers nationwide. On February 21, 2024, UHG revealed that it had fallen victim to this massive data breach, with hackers known as "ALPHV/Blackcat" ("Blackcat") gaining unauthorized access to its networks (the "Data Breach").

5. Blackcat is a prominent cybergroup known for exploiting vulnerabilities in healthcare institutions' internal servers. The group employs ransomware to target and infiltrate "high-value victim institutions." As per the Department of Justice, Blackcat's

---

[2] James Rundle and Catherine Stupp, *Hospitals and Pharmacies Reeling After Change Healthcare Cyberattack*, WSJ.com (Feb. 23, 2024), https://www.wsj.com/articles/hospitals-urged-to-disconnect-from-unitedhealths-hacked-pharmacy-unit-11c9691e (last visited Mar. 11, 2024).

[3] *See* Optum press release at https://www.optum.com/en/about-us/news/page.hub.optuminsight-change-healthcare-combine.html (last visited Mar. 11, 2024); *UnitedHealth Group Form 10-K (Dec.31, 2022),* SEC.

modus operandi typically involves stealing victims' data and encrypting the institution's networks and servers, effectively denying access to them. Subsequently, Blackcat demands a ransom in exchange for providing decryption keys. Additionally, Blackcat pledges not to publish the institution's data on the Dark Web if the ransom is paid. However, despite payments, the compromised data often still surfaces on the Dark Web. Consequently, Blackcat has risen to become the world's second most prolific ransomware-as-a-service variant.[4]

6. Blackcat infiltrated UHG's servers and illicitly obtained extensive sensitive data concerning millions of individuals. This includes identifiable information of active US military and navy personnel, medical and dental records, payment details, claims information, patients' personal data such as phone numbers, addresses, Social Security numbers, emails, as well as insurance records, among other types of Personally Identifiable Information (PHI).[5] Furthermore, Blackcat encrypted sections of UHG's network, rendering them inaccessible.

7. The repercussions of this Data Breach have already caused and will continue to cause significant disruptions in the healthcare sector. Being the largest healthcare insurer, UHG processes a staggering 15 billion transactions annually, impacting a third of all patient records in the United States. However, in an attempt to

[4] *Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant*, DOJ (Dec. 19, 2023), https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant (last visited Mar. 11, 2024).
[5] *MMRG Notifies Patients of Cybersecurity Incident*, BUSINESS WIRE (Feb. 6, 2024, 5:30 PM), https://www.businesswire.com/news/home/20240206060527/en/ (last visited Mar. 11, 2024).

mitigate the ongoing cybersecurity threat, UHG made the decision to take certain systems offline. Consequently, the healthcare industry is now facing immobilization without the functionality of UHG's systems. Patients find themselves stranded in a state of prescription limbo, unable to access essential medications. This situation is particularly distressing for elderly individuals with fixed incomes who rely on insurance for medication expenses, as well as for those with chronic illnesses who face life-threatening consequences without their prescribed medications. The network outage orchestrated by UHG is endangering the health and well-being of millions of Americans.

8. Patients are not the only casualties. The repercussions of the Data Breach are also severely impeding the operations of healthcare providers. According to John Riggi, a national advisor for cybersecurity and risk at the American Hospital Association, "this cyberattack has impacted every hospital in the country to some extent."[6] Numerous providers are encountering difficulties in verifying patient eligibility and coverage, processing claims, and invoicing patients. This predicament particularly affects small and mid-sized practices, leaving them exceptionally vulnerable without the usual cash flow to sustain their operations. Over the past ten days, these healthcare practices have been unable to receive reimbursements from insurers for patient visits. Consequently, without these vital reimbursements, these vulnerable providers cannot afford employee payroll and medical supplies. The combination of untreated patients and debilitated hospitals

[6] Nicole Sganga & Andres Triay, *Cyberattack on UnitedHealth still impacting prescription access: "These are threats to life,"* CBS NEWS (Feb. 29, 2024, 9:00 PM), https://www.cbsnews.com/news/unitedhealth-cyberattack-change-healthcare-prescription-access-still-impacted/. (last visited Mar.11, 2024).

forebodes a grim future.

9. UHG bears responsibility for the Data Breach due to its failure to enact adequate security measures and protocols, as well as its failure to disclose significant information regarding its deficient security practices.

10. Due to UHG's negligence in safeguarding the sensitive information entrusted to it, the Plaintiff and members of the Class have been deprived of the intended protection guaranteed by their agreement with UHG. Consequently, they now encounter substantial risks of medical-related theft, financial fraud, and various forms of identity-related fraud, both presently and in the foreseeable future.

11. Plaintiff initiates this class action lawsuit representing herself and all individuals in a similar situation to address the Defendants' insufficient protection of Class Members' PHI, which it collected and maintained. Further, the lawsuit addresses the Defendants' failure to promptly and adequately notify the Plaintiff and other Class Members about the unauthorized access of their information by an unknown third party, as well as the precise type of information that was accessed.

12. Through this Complaint, the Plaintiff aims to address these damages on behalf of herself and all individuals in similar circumstances whose PHI was accessed during the Data Breach.

13. Plaintiff is seeking remedies that include, but are not limited to, compensatory damages and injunctive relief. This relief encompasses enhancements to the Defendants' data security systems, annual audits, and the provision of adequately funded credit monitoring services by the Defendants.

PARTIES

14. Plaintiff Sandra Groom is a natural person and citizen of Point, Texas.

15. Defendant UnitedHealth Group Incorporated is a Delaware corporation with its principal place of business in Minnetonka, Minnesota.

16. Defendant UnitedHealthcare, Inc. is a Delaware corporation with its principal place of business in Minnetonka, Minnesota.

17. Defendant Optum, Inc. is a Delaware corporation with its principal place of business in Eden Prairie, Minnesota

18. Defendant Change Healthcare, Inc is a Delaware corporation with its principal place of business in Nashville, Tennessee.

JURISDICTION AND VENUE

19. This Court has subject matter jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy exceeds $5 million exclusive of interest and costs. There are more than 100 putative class members and at least some members of the proposed Class have a different citizenship from Defendants. This Court has supplemental jurisdiction over the state law claims pursuant to 28 U.S.C. § 1367 because all claims alleged herein form part of the same case or controversy.

20. This Court has jurisdiction over UHG because it maintains and operates its headquarters in this District and/or is authorized to and does conduct business in this District.

21. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) (1) & (2) because UHG resides in this District and/or a substantial part of the events and omissions

giving rise to this action occurred in this District.

FACTUAL ALLEGATIONS

22. As referenced above, UHG is a healthcare conglomerate consisting of UnitedHealthcare, along with three Optum divisions: Optum Health, OptumInsight, and Optum Rx."[7]

23. As per Optum's website, Optum Health offers direct care services through local medical groups and ambulatory care systems, providing primary, specialty, urgent, and surgical care to nearly 103 million consumers. Optum Health serves a diverse clientele, including employers, health systems, government agencies, and health plans.[8]

24. According to Optum's website, OptumInsight offers a range of solutions including data, analytics, research, consulting, technology, and managed services to hospitals, physicians, health plans, governments, and life sciences companies. This division assists customers in lowering administrative expenses, complying with regulations, enhancing clinical performance, and reimagining operational processes.[9]

25. Optum Rx provides a comprehensive range of pharmacy care services aimed at making medications more accessible and enhancing consumer experiences. Annually, it fills over 1.5 billion adjusted retail, mail, and specialty drug prescriptions. Optum Rx solutions are grounded in evidence-based clinical guidelines. As part of its

[7] *See* FN1, *supra.*
[8] *Optum: Technology and data-enabled care delivery*, UNITEDHEALTH GROUP, https://www.unitedhealthgroup.com/people-and-businesses/businesses/optum.html (last visited Mar. 11, 2024).
[9] *Id.*

regular operations, Optum Rx collects and retains payment and health information from both patients and benefit sponsors.[10]

26. Defendant Change Healthcare operates as a health technology company offering pharmacies and healthcare providers in the United States electronic tools for processing claims and managing essential payment and revenue procedures.

27. Change Healthcare is among the largest prescription medication processors in the United States, managing billing for over 67,000 pharmacies nationwide and facilitating 15 billion healthcare transactions annually.[11]

28. As referenced above, in October 2022, UHG finalized its acquisition of Change Healthcare, aiming to integrate it with OptumInsight.[12]

29. Accordingly, the President of UHG and CEO of Optum said that the combination of Change's and Optum's services "will help streamline and inform the vital clinical, administrative and payment processes on which health care providers and payers depend to serve patients."[13]

30. Therefore, as part of their routine operations, Optum and Change receive and/or retain patients' payment and health insurance details, along with their sensitive health information.

31. As referenced in UHG's most recent annual report submitted to the SEC,

---

[10] *Id.*
[11] *See* FN 2, *supra*.
[12] *See* FN 3, *supra*.
[13] *OptumInsight and Change Healthcare Combine to Advance a More Modern, Information and Technology-Enabled Health Care Platform*, UNITEDHEALTH GROUP (Jan. 6, 2021), https://www.unitedhealthgroup.com/newsroom/2021/2021-01-06-optuminsight-and-change-healthcare-combine.html (last visited Mar. 11, 2024).

UHG "acquired all of the outstanding common shares of Change Healthcare." Consequently, Change Healthcare, just like Optum, is now wholly owned by UHG and operates under the umbrella of UHG's corporate structure.

32. As such, UnitedHealth Group Incorporated is accountable for supervising the cybersecurity practices and protocols of all UHG companies within its corporate framework.

UHG's Privacy Practices

33. As part of its routine operations, UHG retains highly sensitive health information from various sources such as Medicare, pharmacies, healthcare providers, and others. This information comprises patients' complete identities, contact details, Social Security numbers, medical and dental records, payment and claims data, insurance records, and more.

34. Given the extensive amount and sensitive nature of the data they handle, the Defendants maintain privacy policies outlining the usage and disclosure of confidential and personal information. UnitedHealth Group Incorporated, UnitedHealthcare, and Optum adhere to the same "Privacy Policy." They assure their customers that they have implemented "administrative, technical, and physical safeguards" to safeguard patients' information. Their "Social Security Number Protection Policy" explicitly states their commitment to preserving the confidentiality of Social Security numbers received or collected during business operations. They also pledge to limit access to Social Security numbers to lawful purposes and to prohibit unlawful disclosure. Change Healthcare similarly assures that it implements and maintains security measures—organizational,

technical, and administrative—to protect processed data from unauthorized access, destruction, loss, alteration, or misuse. These measures aim to uphold the integrity and confidentiality of data, including personal information.[14]

35. Accordingly, as stated on its website, the Change Healthcare assures:

> We implement and maintain organizational, technical, and administrative security measures designed to safeguard the data we process against unauthorized access, destruction, loss, alteration, or misuse. These measures are aimed at providing on-going integrity and confidentiality of data, including your personal information. We evaluate and update these measures on an ongoing basis. Your Personal Information is only accessible to personnel who need to access it to perform their duties.[15]

36. Throughout their interaction, patients, including the Plaintiff and Class Members, provided the Defendant with their PHI, which the Defendant relies on to conduct its routine business operations.

The Breach

37. On February 21, 2024, in an SEC filing, UnitedHealth Group Incorporated disclosed that a suspected nation-state associated cyber threat actor had accessed some of the Change Healthcare information technology systems. Upon discovering the breach, UnitedHealth Group Incorporated claimed to have proactively isolated the affected systems from other connected systems. Additionally, UnitedHealth Group Incorporated stated that it was collaborating with law enforcement and had reportedly notified customers, clients, and certain government agencies about the breach. The company

[14] *Privacy Notice*, CHANGE HEALTHCARE, https://www.changehealthcare.com/privacy-notice (last visited Mar. 11, 2024).

[15] https://www.changehealthcare.com/privacy-notice (last visited Mar. 11, 2024).

further revealed that the network interruption was specific to Change Healthcare.

38. Approximately one week after the SEC filing went public, Blackcat took responsibility for the breach. Blackcat revealed the extent of the breach, which impacted all Defendants. The group also disclosed that it had managed to extract over 6-TB of highly selective data, which pertained to all Change Health clients with sensitive data processed by the company. Blackcat identified various entities from which it obtained sensitive data, including Medicare, Tricare, CVS-CareMark, Loomis, MetLife, and others.

39. In fact, Blackcat revealed that the extracted data encompasses millions of records, including "active US military/navy personnel PII," medical and dental records, payment details, claims information, patients' personal identifiable information (such as phone numbers, addresses, SSNs, emails, etc.), over 3000 source code files for Change Health solutions, insurance records, and various other data.

40. Considering that Change Healthcare manages 15-billion healthcare transactions annually, equivalent to approximately one in three U.S. patient records, the potential ramifications of the Data Breach are substantial, and its repercussions may persist for many years.

The Breach was Preventable

41. UHG's cybersecurity practices and policies were insufficient and did not meet the industry-standard measures that should have been in place well before the Data Breach occurred. This is particularly notable given that the healthcare sector is often a prime target for cyberattacks, with incidents involving stolen credentials seeing a

significant rise in recent years.

42. Healthcare providers and their affiliates, such as UHG, are particularly attractive targets due to the wealth of sensitive information they gather and retain. This includes patients' financial data, login credentials, insurance details, medical records and diagnoses, as well as personal information of both employees and patients—all highly sought after on underground markets.

43. The risk is so widespread among healthcare providers that on October 28, 2020, the FBI and two federal agencies issued a "Joint Cybersecurity Advisory," cautioning about "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers." The Cybersecurity and Infrastructure Security Agency (CISA), the Department of Health and Human Services (HHS), and the FBI released the advisory to urge healthcare providers to implement "timely and reasonable precautions" to safeguard their networks from these threats.[16]

44. Defendant had the opportunity to avert this Data Breach through various means, including ensuring the proper encryption or protection of their equipment and computer files containing PHI and other sensitive information.

45. To prevent and detect cyberattacks and/or ransomware attacks, the Defendant could and should have implemented the following measures, as recommended by the United States Government:

[16] *Ransomware Activity Targeting the Healthcare and Public Health Sector*, JOINT CYBERSECURITY ADVISORY, https://us-cert.cisa.gov/sites/default/files/publications/AA20-302A_Ransomware%20_Activity_Targeting_the_Healthcare_and_Public_Health_Sector.pdf (last visited Mar. 11, 2024).

i. Implement an awareness and training program to educate patients and individuals about the threat of ransomware and its delivery methods.

ii. Enable strong spam filters to block phishing emails and authenticate inbound email using technologies like SPF, DMARC, and DKIM to prevent email spoofing.

iii. Scan all incoming and outgoing emails for threats and filter executable files from reaching end users.

iv. Configure firewalls to block access to known malicious IP addresses.

v. Regularly patch operating systems, software, and firmware on devices, and consider using a centralized patch management system.

vi. Set up anti-virus and anti-malware programs to conduct automatic scans regularly.

vii. Manage privileged accounts based on the principle of least privilege, restricting administrative access only to users who absolutely need it and limiting its use to when necessary.

viii. Configure access controls with least privilege in mind, ensuring users have only the necessary permissions for file, directory, and network share access.

ix. Disable macro scripts from office files transmitted via email and consider using Office Viewer software for opening Microsoft Office files received via email.

x. Implement Software Restriction Policies (SRP) or similar controls to

prevent programs from executing from common ransomware locations.

xi. Consider disabling Remote Desktop Protocol (RDP) if it is not in use.

xii. Use application whitelisting to only allow systems to execute authorized programs.

xiii. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[17]

46. To prevent and detect cyber-attacks or ransomware attacks, Defendants could and should have implemented the following measures, as recommended by the Microsoft Threat Protection Intelligence Team:

Secure Internet-Facing Assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

Thoroughly Investigate And Remediate Alerts

- Prioritize and treat commodity malware infections as potential full compromise;

Include IT Pros In Security Discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

Build Credential Hygiene

- Use [multifactor authentication] or [network level authentication] and use

[17] *Id.* at 3-4.

strong, randomized, just-in-time local admin passwords;

Apply Principle Of Least-Privilege

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events;

Harden Infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office[Visual Basic for Applications].[18]

47. Considering that Defendant was storing the PHI and other private information of both current and former patients, as well as patients of its clients, it was imperative for the Defendant to implement all of the aforementioned measures to prevent and detect cyberattacks.

48. The Data Breach event indicates that the Defendant inadequately implemented one or more of the aforementioned measures to prevent cyberattacks. This failure led to the Data Breach and, based on available information and belief, exposed the PHI of thousands to tens of thousands of patients, including that of the Plaintiff and Class Members.

49. UHG, being a large entity within the healthcare industry and handling valuable data, should have implemented strong safeguards to detect and thwart any

[18] *See* Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at:* https://www.microsoft.com/en-us/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/ (last visited Mar. 11, 2024).

successful intrusion well before it could escalate to compromising millions of patient files. UHG's failure to uphold industry-standard procedures and policies is unacceptable, particularly considering its awareness of being a prime target for cyberattacks.

Plaintiff's Experiences

50. Plaintiff Sandra Groom is a United Healthcare patient enrolled in Medicare Advantage through UHC Texas.

51. To receive medical treatment, Ms. Groom was obligated to furnish United Healthcare with her sensitive personal information, which included, among other details, her full name, contact information, date of birth, social security number, and private health insurance information.

52. As such, UGH retained various details, including her patient account numbers, health insurance information, medical record identifiers, dates of service, provider names, as well as medical and clinical treatment records.

53. In turn, United Healthcare transmitted her Protected Health Information (PHI) to Optum, which subsequently forwarded it to UHG for the purpose of processing Plaintiff Groom's prescription. UHG then chose to retain Ms. Groom's PHI within its systems.

54. Plaintiff Groom receives a monthly prescription from Optum. In order to receive prescription services from Defendant Optum, she was required to provide UHG and Optum with her patient account numbers, health insurance information, medical record identifiers, dates of service, provider names, as well as medical and clinical treatment records.

55. After February 21, 2024, the Plaintiff became aware that her healthcare provider (United Healthcare) and pharmacy (Optum) were directly involved in the data breach as they were associated with Change Healthcare.

56. Moreover, given that the Data Breach impacted the PHI of patients associated with United Healthcare and Optum, she has dedicated considerable time and effort to investigating the breach and meticulously examining her financial and medical records for any indications of unauthorized activity. She expects to maintain this level of vigilance indefinitely.

UHG's Noncompliance with Federal Law and Regulatory Directives

57. UHG is subject to the regulations set forth in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") as outlined in 45 C.F.R. § 160.102, and is thus obligated to comply with HIPAA Privacy Rule and Security Rule, 45 C.F.R Part 160 and Part 164, Subparts A and E ("Standards for Privacy of Individually Identifiable Health Information"), as well as the Security Rule ("Security Standards for the Protection of Electronic Protected Health Information"), 45 C.F.R. Part 160 and Part 164, Subparts A and C.

58. These regulations set forth national standards aimed at safeguarding patient information, including PHI, which is defined as "individually identifiable health information" that either directly identifies the individual or provides a reasonable basis to believe that the information can be used for identification purposes. This information is held or transmitted by healthcare providers, as per 45 C.F.R. § 160.103.

59. HIPAA restricts the acceptable uses of "protected health information" and

forbids unauthorized disclosures of such information.[19]

60. HIPAA mandates that UHG establish suitable safeguards for this information.[20]

61. HIPAA mandates that UHG must notify individuals in the event of a breach involving unsecured protected health information. This includes instances where the protected health information is not encrypted, making it accessible to unauthorized individuals.[21]

62. Despite these mandates, UHG neglected to fulfill its obligations under HIPAA and its own privacy protocols. Specifically, UHG failed to maintain a sufficient data security system to mitigate the risk of data breaches and cyberattacks, 45 C.F.R. § 164.306(a)(1); adequately safeguard patients' PHI; ensure the confidentiality and integrity of electronically protected health information, 45 C.F.R. § 164.306(a)(1); implement technical policies and procedures for electronic information systems handling electronically protected health information to grant access solely to authorized individuals or software programs, 45 C.F.R. § 164.312(a)(1); implement adequate policies and procedures to prevent, detect, contain, and rectify security violations, 45 C.F.R. § 164.308(a)(1)(i); establish adequate procedures for regularly reviewing records of information system activity, such as audit logs, access reports, and security incident tracking reports, 45 C.F.R. § 164.308(a)(1)(ii)(D); protect against reasonably

[19] *See* 45 C.F.R. § 164.502.
[20] *See* 45 C.F.R. § 164.530(c)(1).
[21] *See* 45 C.F.R. § 164.404; 45 C.F.R. § 164.402.

anticipated uses or disclosures of electronic protected health information not permitted under the privacy rules concerning individually identifiable health information, 45 C.F.R. § 164.306(a)(3); ensure compliance with the rules regarding electronically protected health information security standards by their workforces, 45 C.F.R. § 164.306(a)(4); and adequately train all members of their workforces on the policies and procedures pertaining to protected health information, necessary and appropriate for the members to fulfill their roles and maintain the security of protected health information, 45 C.F.R. § 164.530(b).

63. Moreover, federal agencies have released recommendations and guidelines aimed at mitigating the risks of data breaches for businesses that handle sensitive data. For instance, the Federal Trade Commission ("FTC") has published several guides for businesses, emphasizing the significance of implementing reasonable data security practices, which should inform all business-related decision-making processes.[22]

64. The FTC's publication "Protecting Personal Information: A Guide for Business" outlines essential data security principles and practices for businesses to adopt and adhere to in order to safeguard sensitive data. Among other recommendations, the guidelines suggest that businesses should (a) safeguard the personal customer information they gather and store; (b) appropriately dispose of unnecessary personal information; (c) encrypt information stored on their computer networks; (d) be aware of

[22] *Start with Security*, FTC, https://www.ftc.gov/business-guidance/resources/start-security-guide-business (last visited Mar. 11, 2024).

vulnerabilities in their networks; and (e) establish policies to address security issues. Additionally, the FTC guidelines advise businesses to utilize an intrusion detection system, monitor incoming traffic for unusual activity, keep an eye out for large amounts of data being transmitted from their system, and have a response plan prepared in the event of a breach.[23]

65. Furthermore, the FTC advises companies to restrict access to sensitive data, enforce the use of complex passwords on networks, utilize industry-standard security methods, monitor the network for suspicious activity, and ensure that third-party service providers have implemented adequate security measures. This aligns with the guidance offered by the FBI, HHS, and the principles outlined in the CISA 2020 guidance.

66. Accordingly, the FTC has taken enforcement actions against businesses that have inadequately protected customer information, considering the failure to implement reasonable and appropriate measures to safeguard against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45. The Orders stemming from these actions provide additional guidance on the steps businesses must take to fulfill their data security responsibilities.[24]

67. As such, UHG was fully aware of its responsibility to adopt and apply

[23] *Protecting Personal Information*, FTC, https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf (last visited Mar. 11, 2024).
[24] *Privacy and Security Enforcement*, FTC, https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement (last visited Mar. 11, 2024).

reasonable measures to safeguard the PHI of its patients. However, it failed to adhere to these fundamental recommendations and guidelines, which could have averted this breach. UHG's failure to implement reasonable measures to prevent unauthorized access to patient information constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

Common Injuries & Damages

68. The PHI compromised in the Data Breach is highly sought after and holds significant value on underground markets. It can be exploited for various malicious activities, including identity fraud, particularly medical-related identity theft and fraud, which is recognized as one of the most perilous and financially burdensome forms of identity theft.

69. Tom Kellermann, the chief cybersecurity officer of Carbon Black, a cybersecurity company, asserts that "Health information is a treasure trove for criminals because, by compromising it, stealing it, or selling it, they gain access to seven to ten personal identifying characteristics of an individual." Consequently, complete medical records of a patient can fetch up to $1,000 on the dark web, whereas credit card numbers and Social Security numbers may cost as little as $5 or less.[25]

70. According to Paul Nadrag, a software developer specializing in medical device integration and data technology at Capsule Technologies, the price discrepancy

[25] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last visited Mar. 11, 2024).

between medical records and credit card numbers is attributed to perceived value. While a credit card number can be swiftly canceled, medical records contain a wealth of immutable data points, including a patient's comprehensive medical and behavioral health history, demographics, health insurance, and contact details. Once obtained, cybercriminals often leverage connections within a dark web criminal network, typically involved in drug trafficking and money laundering. These networks eagerly purchase medical records to facilitate various illicit activities, such as unlawfully acquiring prescription medications, submitting fraudulent medical claims, or perpetrating identity theft by opening unauthorized credit cards and obtaining fraudulent loans.[26]

71. While federal law typically limits an individual's liability for fraudulent charges on a credit card to $50, there exist no such safeguards for stolen medical identities. According to a 2015 survey on medical identity theft conducted by the Ponemon Institute, victims of medical identity theft incurred an average of $13,500 in out-of-pocket expenses to resolve the crime. Often, this stolen information was utilized to access medical services or treatments (59%), obtain prescription drugs (56%), or receive Medicare and Medicaid benefits (52%). Only 14% of respondents reported that identity thieves used the information to acquire fraudulent credit accounts, underscoring the significantly more lucrative nature of the medical information market.[27]

---

[26] *See* Paul Nadrag, *Industry Voices—Forget credit card numbers. Medical records are the hottest items on the dark web*, FIERCE HEALTHCARE (Jan. 26, 2021, 3:55 PM), https://www.fiercehealthcare.com/hospitals/industry-voices-forget-credit-card-numbers-medical-records-are-hottest-items-dark-web. (last visited Mar. 11, 2024).

[27] *Fifth Annual Study on Medical Identity Theft*, PONEMON INSTITUTE (Feb. 2015), https://static.nationwide.com/static/2014_Medical_ID_Theft_Study.pdf?r=65 (the "Ponemon

72. According to the Ponemon study, individuals who successfully resolved the crime spent an average of over 200 hours on tasks such as collaborating with their insurer or healthcare provider to ensure the security of their personal medical credentials, confirming the accuracy of their personal health information, medical invoices, claims, and electronic health records. Furthermore, the study revealed that medical identity theft can adversely affect one's reputation, with 45% of respondents indicating that it impacted their reputation, primarily due to embarrassment stemming from the disclosure of sensitive personal health conditions. Additionally, 19% reported missing out on employment opportunities as a consequence.[28]

73. Furthermore, victims often face significant delays in detecting instances of medical-related identity theft or fraud, which can span several months or even years due to challenges associated with accessing medical records and healthcare statements. For instance, according to the FTC, individuals may only realize their identity has been compromised when they: (a) receive bills for medical services they never received, (b) are contacted by debt collectors regarding medical debt they do not owe; (c) encounter unfamiliar medical collection notices on their credit reports; (d) discover incorrect listings of office visits or treatments on their explanation of benefits; (e) receive notifications from their health plan indicating that they have exceeded their benefits limit; (f) Experience insurance denials due to medical records displaying conditions

Study") (last visited Mar. 11, 2024).
[28] *Id.*

they do not have.[29]

74. Arguably the most perilous aspect of medical identity theft is the potential for misdiagnoses or erroneous treatment. Ann Patterson, a senior vice president of the Medical Identity Fraud Alliance, highlights this concern, stating that "[a]bout 20 percent of victims have reported receiving incorrect diagnoses or treatments, or experiencing delays in care due to the confusion stemming from identity theft in their records." This sentiment is echoed by the Ponemon study, which underscores that "many respondents are vulnerable to additional theft or inaccuracies in healthcare records, which could compromise medical treatments and diagnoses."[30]

75. As Tom Kellermann explains, "Traditional criminals recognize the leverage of coercion and extortion. Possessing healthcare information, particularly details about a sexually transmitted disease or terminal illness, can be wielded to coerce or extort individuals into compliance." This form of identity theft extends over the long term, as fraudsters amalgamate a victim's various data points, including publicly accessible information or details revealed in other data breaches, to fabricate new identities, initiate fraudulent credit accounts, or perpetrate tax fraud, all of which may require years to rectify.[31]

76. Numerous individuals impacted by the Data Breach have likely suffered

[29] *See Medical Identity Theft, FAQs for Health Care Providers and Health Plans*, FTC.GOV, https://www.ftc.gov/system/files/documents/plain-language/bus75-medical-identity-theft-faq-health-care-health-plan.pdf (last visited Mar. 11, 2024).
[30] *See* FN 27, *supra*.
[31] Andrew Steger, *What Happens to Stolen Healthcare Data?*, HEALTHTECH (Oct. 30, 2019), https://healthtechmagazine.net/article/2019/10/what-happens-stolen-healthcare-data-perfcon (last visited Mar. 11, 2024).

substantial damages, encompassing medical-related identity theft and fraud, among other consequences. Plaintiffs and members of the affected class have additionally invested considerable resources—both financially and in terms of time and effort—addressing the aftermath of the Data Breach. This may involve acquiring credit monitoring services, scrutinizing financial and healthcare records, monitoring credit reports, and dedicating time and energy to identifying unauthorized activities.

77. It is understandable that identity theft imposes a significant emotional burden on its victims. The findings of the 2017 Identity Theft Resource Center survey vividly illustrate the emotional distress experienced by those affected by identity theft wherein: 75% of respondents reported feeling severely distressed; 67% reported anxiety; 66% reported feelings of fear related to personal financial safety; 37% reported fearing for the financial safety of family members; 24% reported fear for their physical safety; 15.2% reported a relationship ended or was severely and negatively impacted by the identity theft; 7% reported feeling suicidal.[32]

78. The dark web consists of numerous distinct repositories housing stolen information, which can be aggregated or accessed by various criminal actors for diverse fraudulent purposes. With each data breach, the probability rises that a victim's personal information will be exposed to additional individuals seeking to exploit it to the detriment of the victim.

[32] *Identity Theft: The Aftermath 2017*, ITRC, https://www.idtheftcenter.org/wp-content/uploads/images/page-docs/Aftermath_2017.pdf (last visited Mar. 11, 2024).

79. Due to the extensive range of injuries stemming from the Data Breach, the Plaintiff and members of the class have experienced and will continue to endure economic losses and other tangible harms, warranting damages. These damages include, but are not restricted to, the following: unauthorized disclosure of confidential data, depreciation of data security assurances, identity theft and fraud risks, expenses for identity theft detection and prevention, emotional distress, and costs for credit monitoring and identity theft protection services, unauthorized charges, restricted access to financial accounts, associated costs such as missed payments and late fees, lowered credit scores due to fraudulent activities, time and productivity losses addressing breach consequences, and ongoing risks of fraud and identity theft from compromised personal information.

80. To make matters worse, there might be a significant delay between the theft of personal information and its fraudulent use. According to the Government Accountability Office, findings suggest that stolen data could be stored for over a year before being exploited for identity theft. Additionally, once the data is sold or circulated online, fraudulent activities may persist for years. Consequently, studies aiming to quantify the impact of data breaches may not be able to entirely disregard potential future harm. [33]

81. Healthcare providers with strong data security measures are esteemed more by patients, enabling them to charge higher fees. Therefore, if patients were aware of UHG's inadequate PHI protection, they might have avoided its affiliated services or paid

[33] PERSONAL INFORMATION: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft is Limited; However, the Full Extent is Unknown, GAO, http://www.gao.gov/new.items/d07737.pdf (last visited Mar. 11, 2024).

less. Consequently, Plaintiff and Class members didn't get the service value they paid for, as they paid for services they didn't fully receive.

82. UHG's failure to fulfill its obligations prompts Plaintiff and Class members to pursue compensation in the form of identity protection services. This seeks to address both current damages and the ongoing elevated risk resulting from UHG's misconduct. The aim is to restore Plaintiff and Class members as closely as possible to their pre-damage state, specifically regarding the inadequate protection of their PHI.

83. Further, Plaintiff and Class members seek to regain the value of the unauthorized access to their PHI facilitated by UHG's wrongful actions. Plaintiff and Class Members possess a defendable property interest in their PHI.

Loss Of Time To Mitigate Risk

84. Due to the acknowledged risk of identity theft, it is expected that a reasonable person would take measures and allocate time to confront the perilous situation. This entails understanding the breach, undertaking actions to mitigate the risk of falling victim to identity theft or fraud, and reviewing accounts or credit reports. Neglecting to dedicate time to these tasks could heighten the individual's exposure to significant financial harm. Consequently, the valuable resource and asset of time would have been squandered.

85. Defendants' failure to promptly notify the Plaintiff and Class Members of the Data Breach has hindered mitigation efforts, adding additional burdens. This situation is worsened by the Defendants' inadequate communication about the incident and their failure to detail preventive measures for future harm in a timely and comprehensive manner. Essentially, the Plaintiff and Class Members are left to handle

the situation on their own.

86. Consequently, Plaintiff and Class Members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach.

87. Plaintiff's mitigation efforts are consistent with the U.S. Government Accountability Office that released a report in 2007 regarding data breaches ("GAO Report") in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[34]

88. Plaintiff's mitigation efforts are also consistent with the steps that FTC recommends that data breach victims take several steps to protect their personal and financial information after a data breach, including: contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for seven years if someone steals their identity), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[35]

89. For those Class Members who experience actual identity theft and fraud, the United States Government Accountability Office issued a report in 2007 concerning data breaches ("GAO Report"). In this report, it was highlighted that

[34] *See* United States Government Accountability Office, GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (June 2007), https://www.gao.gov/products/gao-07-737 (last visited Mar. 11, 2024).

[35] *See* Federal Trade Commission, *Identity Theft.gov*, https://www.identitytheft.gov/Steps (last visited Mar. 11, 2024).

victims of identity theft would confront "significant costs and time to rectify the harm to their reputation and credit history.[36]

Diminution Value Of PHI

90. PHI is a valuable property right. Its value is axiomatic, considering the value of Big Data, especially health related data, in corporate America and the consequences of cyber thefts include heavy prison sentences. Even this obvious risk to reward analysis illustrates beyond doubt that PHI has considerable market value.

91. A thriving and robust legitimate market for PHI exists. In 2019, the data brokering industry boasted an approximate worth of $200 billion.[37]

92. In fact, the data marketplace is so sophisticated that consumers can actually sell their non-public information directly to a data broker who in turn aggregates the information and provides it to marketers or app developers.[38]

93. Due to the Data Breach, the PHI of the Plaintiff and Class Members, possessing inherent market value in both legitimate and illicit markets, has suffered degradation and diminishment due to its compromise and unauthorized dissemination. This transfer of value transpired devoid of any compensation rendered to the Plaintiff or Class Members for their property, resulting in an economic loss. Furthermore, the PHI is now readily accessible, and the exclusivity of the Data has been eroded, thereby

[36] *See* "Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown," p. 2, U.S. Government Accountability Office, June 2007, https://www.gao.gov/new.items/d07737.pdf (last visited Mar. 11, 2024) ("GAO Report").
[37] *See* https://www.latimes.com/business/story/2019-11-05/column-data-brokers (last visited Mar. 11, 2024).
[38] *See* https://datacoup.com/ (last visited Mar. 11, 2024).

resulting in further loss of value.

94. Given the foregoing, the information compromised in the Data Breach holds considerably greater value compared to the loss of credit card information in a retailer data breach. In the latter scenario, victims have the option to cancel or close credit and debit card accounts. However, the information compromised in this Data Breach cannot be simply "closed" and is challenging, if not impossible, to alter.

95. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

96. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PHI of Plaintiff and Class Members, and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

97. The injuries sustained by the Plaintiff and Class Members were directly and proximately attributable to the Defendants' failure to establish or uphold sufficient data security measures for their PHI.

Future Cost of Credit and Identity Theft Monitoring is Reasonable and Necessary

98. Given the type of targeted attack in this case and sophisticated criminal activity, the type of PHI involved, and the volume of data obtained in the Data Breach, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals

intending to utilize the PHI for identity theft crimes.

99. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that his or her personal information was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

100. Consequently, Plaintiff and Class Members are at a present and continuous risk of fraud and identity theft for many years into the future.

101. The retail cost of credit monitoring and identity theft monitoring can cost around $200 a year per Class Member. This is a reasonable and necessary cost to monitor to protect Class Members from the risk of identity theft that arose from Defendants' Data Breach. This is a future cost for a minimum of five years that Plaintiff and Class Members would not need to bear but for Defendants' failure to safeguard their PHI.

Loss Of The Benefit Of The Bargain

102. Defendants' poor data security deprived Plaintiff and Class Members of the benefit of their bargain. When agreeing to pay Defendants and/or its clients for the provision of medical services, Plaintiff and other reasonable consumers understood and expected that they were, in part, paying for the service and necessary data security to protect the PHI, when in fact, Defendants did not provide the expected data security. Accordingly, Plaintiff and Class Members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendants and/or its clients.

CLASS ACTION ALLEGATIONS

103. Plaintiff seeks relief both personally and as a representative for all those in similarly situated. Pursuant to Federal Rule of Civil Procedure 23, Plaintiff initiates this action on behalf of herself and a defined class, consisting of:

> **All persons in the United States whose personal health information was compromised as a result of the Data Breach announced by UnitedHealth Group Incorporated in February 2024 (the "Class").**

104. Excluded from the Class are Defendants and its parents or subsidiaries, any entities in which it has a controlling interest, as well as its officers, directors, affiliates, legal representatives, heirs, predecessors, successors, and assigns. Also excluded is any Judge to whom this case is assigned as well as their judicial staff and immediate family members.

105. Plaintiff reserves the right to modify or amend the definition of the proposed Class, as well as add subclasses, before the Court determines whether certification is appropriate.

106. The proposed Class meets the criteria for certification under Fed. R. Civ. P. 23(a), (b)(2), and (b)(3).

107. Numerosity. The Class Members are so numerous that joinder of all members is impracticable. Although the precise number of such persons is unknown to Plaintiff and exclusively in the possession of Defendants, upon information and belief, thousands of individuals were impacted in the Data Breach.

108. Commonality. There are questions of law and fact common to the Class which predominate over any questions affecting only individual Class Members. These

common questions of law and fact include, without limitation:

a. Whether Defendants engaged in the conduct alleged herein;

b. Whether Defendants' conduct violated the HIPAA;

c. When Defendants learned of the Data Breach;

d. Whether Defendants' response to the Data Breach was adequate;

e. Whether Defendants unlawfully lost or disclosed Plaintiff's and Class Members' PHI;

f. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the PHI compromised in the Data Breach;

g. Whether Defendants' data security systems prior to and during the Data Breach complied with applicable data security laws and regulations;

h. Whether Defendants' data security systems prior to and during the Data Breach were consistent with industry standards;

i. Whether Defendants owed a duty to Class Members to safeguard their PHI;

j. Whether Defendants breached its duty to Class Members to safeguard their PHI;

k. Whether hackers obtained Class Members' PHI via the Data Breach;

l. Whether Defendants had a legal duty to provide timely and accurate notice of the Data Breach to Plaintiff and the Class Members;

m. Whether Defendants breached its duty to provide timely and accurate notice of the Data Breach to Plaintiff and Class Members;

n. Whether Defendants knew or should have known that its data security systems and monitoring processes were deficient;

o. What damages Plaintiff and Class Members suffered as a result of Defendants' misconduct;

p. Whether Defendants' conduct was negligent;

q. Whether Defendants were unjustly enriched;

r. Whether Plaintiff and Class Members are entitled to compensatory damages, punitive damages, and/or statutory or civil penalties as a result of the Data Breach;

a. Whether Plaintiff and Class Members are entitled to additional credit or identity monitoring and monetary relief; and

b. Whether Plaintiff and Class Members are entitled to equitable relief, including restitution, disgorgement, and/or the establishment of a constructive trust.

109. Typicality. Plaintiff's claims are typical of those of other Class Members because Plaintiff's PHI, like that of every other Class Member, was compromised in the Data Breach. Plaintiff's claims are typical of those of the other Class Members because, inter alia, all Class Members were injured through the common misconduct of Defendants. Plaintiff is advancing the same claims and legal theories on behalf of himself and all other Class Members, and there are no defenses that are unique to Plaintiff. The claims of Plaintiff and those of Class Members arise from the same operative facts and are based on the same legal theories.

110. Adequacy of Representation. Plaintiff will fairly and adequately represent and protect the interests of Class Members. Plaintiff's counsel is competent and experienced in litigating class actions, including data privacy litigation of this kind.

111. Predominance. Defendants have engaged in a common course of conduct toward Plaintiff and Class Members in that all of Plaintiff's and Class Members' data was stored on the same computer systems and unlawfully accessed and exfiltrated in the same way. The common issues arising from Defendants' conduct affecting Class Members set out above predominate over any individualized issues. Adjudication of these common issues in a single action has important and desirable advantages of judicial economy.

112. Superiority. A Class action is superior to other available methods for the fair and efficient adjudication of this controversy and no unusual difficulties are likely to be encountered in the management of this class action. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a Class action, most Class Members would likely find that the cost of litigating their individual claims is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual Class Members would create a risk of inconsistent or varying adjudications with respect to individual Class Members, which would establish incompatible standards of conduct for Defendants. In contrast, conducting this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class Member.

113. Class certification is also appropriate under Fed. R. Civ. P. 23(b)(2). Defendants has acted and/or refused to act on grounds generally applicable to the Class such that final injunctive relief and/or corresponding declaratory relief is appropriate as to the Class as a whole.

114. Finally, all members of the proposed Class are readily ascertainable. Defendants has access to the names and addresses and/or email addresses of Class Members affected by the Data Breach. Class Members have already been preliminarily identified and sent Notice of the Data Breach by Defendants.

COUNT I
Negligence
(On Behalf of Plaintiff and the Class)

115. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1 through 114.

116. As a prerequisite for receiving healthcare services and carrying out UHG's insurer duties related to patient medical treatments, UHG mandated the provision of PHI from Plaintiff and class members. UHG retained this information both for facilitating health insurance services and for commercial purposes.

117. UHG was obligated to exercise reasonable care in safeguarding Plaintiff and class members' PHI against unauthorized access or disclosure. This duty was explicitly recognized in its privacy policies, where UHG pledged not to disclose PHI, including SSNs, without authorization, and committed to compliance with all federal laws and regulations.

118. UHG was obligated to provide Plaintiff and class members with sufficient

data security, in line with industry norms, to guarantee that UHG's systems and networks effectively safeguarded the PHI.

119. Pursuant to HIPAA, UHG held a special relationship with Plaintiff and class members, who relied on UHG to adequately protect their confidential personal, financial, and medical data.

120. Accordingly, Defendants' obligation to exercise reasonable care in safeguarding PHI stems from the parties' relationship, as well as common law and federal regulations, including the HIPAA provisions mentioned earlier, along with UHG's internal policies and commitments concerning privacy and data security.

121. UHG was aware of the inherent risks associated with collecting and storing PHI in a centralized location, its susceptibility to network attacks, and the critical importance of implementing sufficient security measures.

122. UHG breached its duty to Plaintiff and class members in numerous ways, including but not limited to: failing to exercise reasonable care and implement adequate security measures to protect their PHI, neglecting industry-standard data security protocols, disregarding its own privacy policies, violating regulations safeguarding the PHI during the Data Breach period, inadequately monitoring and ensuring the security of UHG's network and systems, and failing to promptly identify the compromised PHI.

123. The compromise of Plaintiff and class members' PHI wouldn't have occurred but for UHG's wrongful and negligent breach of its duties.

124. UHG's failure to implement adequate security measures to safeguard the sensitive PHI of Plaintiff and class members, as detailed in this Complaint, facilitated

conditions ripe for a foreseeable criminal act—specifically, the unauthorized access and duplication of PHI by third parties without authorization.

125. Considering that healthcare providers and their affiliates are prominent targets for cyberattacks, Plaintiff and class members constitute a foreseeable and identifiable group that faced elevated risks of PHI misuse or disclosure if not adequately protected by UHG.

126. As a direct consequence of UHG's actions, Plaintiff and class members will suffer damages including: (i) the loss of rental or usage value of their PHI; (ii) the unauthorized disclosure of their PHI to unauthorized third parties; (iii) expenses incurred for prevention, detection, and recovery from identity theft, fraud, and unauthorized PHI use; (iv) lost opportunity costs associated with addressing and mitigating the present and future consequences of the Data Breach, including research efforts on prevention, detection, contestation, and recovery from fraud and identity theft; (v) the time, effort, and expenses related to placing fraud alerts or credit report freezes; (vi) anxiety, emotional distress, loss of privacy, and other economic and non-economic losses; (vii) the ongoing risk to their PHI, which remains in UHG's possession and susceptible to further unauthorized disclosures unless appropriate and adequate protection measures are taken; (viii) future expenditures of time, effort, and money to prevent, detect, contest, and rectify the ongoing consequences of compromised PHI throughout their lifetimes; and (ix) any nominal damages that may be awarded.

127. Additionally, as a direct and proximate result of Defendants' negligence, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of

their PII, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fails to undertake appropriate and adequate measures to protect the PHI in its continued possession.

COUNT II
Negligence *Per Se*
(On Behalf of Plaintiff and the Class)

128. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1 through 127.

129. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by Defendants of failing to use reasonable measures to protect PHI. Various FTC publications and orders also form the basis of Defendants' duty.

130. Defendants violated Section 5 of the FTC Act (and analogous state laws) by neglecting to implement reasonable measures to safeguard PHI and by failing to adhere to industry standards. Defendants' actions were notably unreasonable, considering the type and volume of PHI acquired and stored, as well as the foreseeable ramifications of a data breach on Defendants' systems.

131. UHG falls under the purview of HIPAA, as per 45 C.F.R. § 160.102, and thus is mandated to adhere to all rules and regulations outlined in 45 C.F.R. Parts 160 and 164.

132. Security and Privacy" are governed by 45 C.F.R. Part 164, where Subpart A offers "General Provisions," Subpart B regulates "Security Standards for the Protection of Electronic Protected Health Information," Subpart C outlines

requirements for "Notification in the Case of Breach of Unsecured Protected Health Information," and Subpart E governs the "Privacy of Individually Identifiable Health Information."

133. According to 45 C.F.R. § 164.104, the "standards, requirements, and implementation specifications adopted under this part" are applicable to covered entities and their business associates, including UHG.

134. UHG is required by HIPAA to guarantee the "confidentiality, integrity, and availability of all electronic protected health information" it handles and to safeguard against anticipated threats or hazards to the security or integrity of such information, as outlined in 45 C.F.R. § 164.306.

135. UHG breached HIPAA regulations by failing to comply with and meet the mandated standards delineated in 45 C.F.R. §§ 164.308, 164.310, 164.312, 164.314, and 164.316.

136. Defendants' duty to use reasonable security measures under HIPAA required Defendants to "reasonably protect" confidential data from "any intentional or unintentional use or disclosure" and to "have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information." 45 C.F.R. § 164.530(c)(l). Some or all of the healthcare and/or medical information at issue in this case constitutes "protected health information" within the meaning of HIPAA.

137. Defendants violated HIPAA (and analogous state statutes) by neglecting to employ reasonable measures to safeguard PHI and by failing to adhere to industry

standards.

138. Defendants' violation of Section 5 of the FTC Act and HIPAA (and similar state statutes) constitutes negligence *per se.*

139. Class members are individuals falling within the category of persons intended to be protected by Section 5 of the FTC Act and HIPAA (along with comparable state statutes).

140. Further, the harm involved in this Data Breach aligns with the type of harm intended to be prevented by the FTC Act and HIPAA (as well as comparable state statutes). In fact, the FTC has initiated over fifty enforcement actions against businesses that, due to their failure to implement reasonable data security measures and refrain from engaging in unfair and deceptive practices, caused harm similar to that experienced by Plaintiff and Class Members.

141. But for Defendants' wrongful and negligent breach of duties owed to Plaintiff and the Class, the PHI of Plaintiff and the Class would not have been compromised.

142. There is a close causal connection between Defendants' failure to implement security measures to protect the PHI of Plaintiff and the Class and the harm, or risk of imminent harm, suffered by Plaintiff and the Class. The PHI of Plaintiff and the Class was lost and accessed as the proximate result of Defendants' failure to exercise reasonable care in safeguarding such PHI by adopting, implementing, and maintaining appropriate security measures.

143. As a direct and proximate result of Defendants' negligence per se, Plaintiff

and the Class have incurred and will continue to endure various forms of harm, including but not limited to: (i) invasion of privacy; (ii) theft of their PHI; (iii) depreciation or loss of value of PHI; (iv) expended time and opportunity costs associated with mitigating the actual repercussions of the Data Breach; (v) deprivation of the expected benefits from the agreement; (vi) missed opportunities and costs incurred while trying to mitigate the actual consequences of the Data Breach; (vii) statutory damages; (viii) nominal damages; and (ix) the persistent and heightened risk to their PHI, which: (a) remains unencrypted and vulnerable to unauthorized access and misuse by third parties; and (b) continues to be backed up in Defendants' possession, subjecting it to further unauthorized disclosures as long as Defendants neglects to implement appropriate and sufficient protective measures for the PHI.

144. As a direct and proximate result of Defendants' negligence per se, Plaintiff and the Class have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

145. Additionally, as a direct and proximate result of Defendants' negligence per se, Plaintiff and the Class have suffered and will suffer the continued risks of exposure of their PHI, which remain in Defendants' possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PHI in its continued possession.

146. Plaintiff and Class Members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

147. Defendants' negligent conduct is ongoing, in that it still holds the PHI of Plaintiff and Class Members in an unsafe and insecure manner.

COUNT III

Breach Of Implied Contract

(On Behalf of Plaintiff and the Class)

148. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1 through 147.

149. Plaintiff and Class Members were required to provide their PHI to Defendants as a condition of receiving services from Defendants and/or its clients.

150. Plaintiff and the Class entrusted their PHI to Defendants. In so doing, Plaintiff and the Class entered into implied contracts with Defendants by which Defendants agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiff and the Class if their data had been breached and compromised or stolen.

151. Implicit in the agreement between Plaintiff, Class Members, and the Defendants regarding the provision of PHI, which Plaintiff and Class Members were required to provide to Defendants, were the following obligations for the Defendants: (a) restrict the use of such PHI solely for business purposes, (b) implement reasonable measures to safeguard the PHI, (c) prevent unauthorized disclosures of the PHI, (d) promptly and adequately notify Plaintiff and Class Members of any unauthorized access and/or theft of their PHI, (e) reasonably safeguard and protect the PHI of Plaintiff and Class Members from unauthorized disclosure or use, and (f) maintain the PHI under

conditions ensuring its security and confidentiality.

152. The mutual understanding and intent between Plaintiff, Class Members, and Defendants are evident through their conduct and ongoing business interactions.

153. Defendants solicited, offered, and invited Plaintiff and Class Members to provide their PHI as part of Defendants' regular business practices. Plaintiff and Class Members accepted Defendants' offers and provided their PHI to Defendants.

154. In accepting the PHI of Plaintiff and Class Members, Defendants understood and agreed that it was required to reasonably safeguard the PHI from unauthorized access or disclosure.

155. On information and belief, at all relevant times Defendants promulgated, adopted, and implemented written privacy policies whereby it expressly promised Plaintiff and Class Members that it would only disclose PHI under certain circumstances, none of which relate to the Data Breach.

156. On information and belief, Defendants further promised to comply with industry standards and to make sure that Plaintiff's and Class Members' PHI would remain protected.

157. When entering into these implied contracts, Plaintiff and Class Members reasonably believed and anticipated that Defendants' data security practices adhered to pertinent laws and regulations and aligned with industry standards.

158. Plaintiff and Class Members paid money to Defendants with the reasonable belief and expectation that Defendants would use part of its earnings to obtain adequate data security. Defendant failed to do so.

159. Plaintiff and Class Members would not have entrusted their PHI to Defendants in the absence of the implied contract between them and Defendant to keep their information reasonably secure.

160. Plaintiff and Class Members would not have entrusted their PHI to Defendants in the absence of their implied promise to monitor their computer systems and networks to ensure that it adopted reasonable data security measures.

161. Plaintiff and Class Members fully and adequately performed their obligations under the implied contracts with Defendant.

162. Defendant breached the implied contracts it made with Plaintiff and the Class by failing to safeguard and protect their personal information, by failing to delete the information of Plaintiff and the Class once the relationship ended, and by failing to provide accurate notice to them that personal information was compromised as a result of the Data Breach.

163. As a direct and proximate result of Defendants' breach of the implied contracts, Plaintiff and Class Members sustained damages, as alleged herein, including the loss of the benefit of the bargain.

164. Plaintiff and Class Members are entitled to compensatory, consequential, and nominal damages suffered as a result of the Data Breach.

COUNT IV
Unjust Enrichment
(On Behalf of Plaintiff and the Class)

165. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1 through 164.

166. This count is pleaded in the alternative to Plaintiff's breach of implied contract claim above (Count III).

167. Plaintiff and class members possess both legal and equitable rights to their PHI entrusted to, collected by, and held by UHG, which was compromised in the Data Breach. This information holds intrinsic value.

168. Plaintiff and Class Members conferred a monetary benefit through payments for medical and healthcare services, including those indirectly remitted to UHG by Plaintiff and class members.

169. Defendants were fully aware that Plaintiff and Class Members provided it with a benefit in the form of their PHI, as well as payments made on their behalf, which were essential for receiving services. Defendants acknowledged and welcomed this benefit, profiting from these transactions and utilizing the PHI of Plaintiff and Class Members for business purposes.

170. Upon information and belief, Defendants' funds its data security measures entirely from its general revenue, including payments on behalf of or for the benefit of Plaintiff and Class Members.

171. As such, the fees for medical and healthcare services paid by Plaintiff and class members, whether directly or indirectly, should have been allocated by UHG to cover a portion of the administrative expenses related to implementing reasonable data privacy and security practices and procedures.

172. Defendants, however, failed to secure Plaintiff's and Class Members' PHI and, therefore, did not provide adequate data security in return for the benefit

Plaintiff and Class Members provided.

173. Defendants would not be able to carry out an essential function of its regular business without the PHI of Plaintiff and Class Members and derived revenue by using it for business purposes. Plaintiff and Class Members expected that Defendants or anyone in Defendants' position would use a portion of that revenue to fund adequate data security practices.

174. Due to UHG's actions, Plaintiff and class members experienced tangible losses as detailed herein. In accordance with principles of fairness and equity, UHG should be required to disgorge all illegitimate or unjust gains acquired from Plaintiff and class members into a common fund. This includes compensation equal to the disparity in value between medical and healthcare services encompassing the implementation of reasonable data privacy and security practices, which Plaintiff and class members paid for, and the services lacking such measures that they actually received.

175. Under these principles of equity and fairness, Defendants should not be allowed to keep the money obtained unlawfully from Plaintiff and Class Members, as Defendants neglected to enforce necessary data management and security measures required by industry standards.

176. Plaintiff and Class Members have no adequate remedy at law.

177. Defendants should be ordered to return, either into a common fund or a constructive trust, the profits obtained unjustly from Plaintiff and Class Members for their benefit. Alternatively, Defendants should be required to reimburse Plaintiff and Class

Members for any excess amounts paid for Defendants' services.

COUNT V
Declaratory Judgment
(On Behalf of Plaintiff and the Class)

178. Plaintiff repeats and re-alleges each and every factual allegation contained in paragraphs 1 through 177.

179. Pursuant to the Declaratory Judgment Act, 28 U.S.C. §§ 2201, et seq., this Court possesses the authority to issue a judgment clarifying the rights and legal relationships of the involved parties and provide any additional essential remedies. Additionally, the Court holds expansive power to prohibit actions, such as those here, that are tortious and contravene the terms of the federal statutes delineated in this Complaint.

180. In the aftermath of the Data Breach, a genuine dispute has emerged concerning UHG's existing and future obligations under common law and other regulations to reasonably protect PHI. This includes questioning whether UHG currently upholds data security measures sufficient to safeguard Plaintiff and class members against potential cyberattacks and data breaches that might jeopardize their PHI.

181. UHG retains PHI related to Plaintiff and class members, leaving their information vulnerable to further breaches due to UHG's persistently inadequate data security measures. Consequently, Plaintiff and class members endure ongoing harm from the compromise of their PHI and face an ongoing risk of future breaches compromising their information.

182. Plaintiff seeks a declaration that: (a) UHG's current data security measures fail to meet its obligations and duty of care; and (b) to fulfill its obligations and duty of

care, (1) UHG must establish policies and procedures ensuring that entities with whom it shares sensitive personal information maintain reasonable, industry-standard security measures and comply with these policies and procedures; (2) UHG must: (i) securely purge, delete, or destroy Plaintiff's and class members' PHI if no longer necessary for essential business functions to prevent further theft; and (ii) adopt and maintain reasonable, industry-standard security measures, including, but not limited to: (a) engaging third-party security auditors/penetration testers and internal security personnel to conduct periodic testing, including simulated attacks, penetration tests, and audits on UHG's systems, with prompt correction of identified issues; (b) employing third-party security auditors and internal personnel for automated security monitoring; (c) auditing, testing, and training security personnel on new or modified procedures; (d) encrypting and segmenting PHI, implementing firewalls and access controls to prevent hackers from accessing other system areas in case of compromise; (e) securely purging, deleting, and destroying unnecessary PHI; (f) conducting regular database scanning and security checks; (g) providing regular employee education on best security practices; (h) implementing multi-factor authentication and Principle of Least Privilege to combat system-wide cyberattacks; and (i) continuously training internal security personnel to identify and contain breaches and respond effectively to breaches.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff prays for judgment as follows:

A. For an Order certifying this action as a class action under Rule 23 of the Federal Rules of Civil Procedure, appoint Plaintiff as the class

representative, and appoint Plaintiff's counsel as Class Counsel;

B. For a permanent injunctive relief, restraining UHG from persisting in the illegal actions, omissions, and practices outlined herein;

C. For an award Plaintiff and Class Members compensatory, consequential, and general damages, including nominal damages as appropriate, for each count as allowed by law in an amount to be determined at trial;

D. For an award of statutory damages, trebled, and/or punitive or exemplary damages, to the extent permitted by law.

E. For an Order of order disgorgement and restitution of all earnings, profits, compensation, and benefits received by UHG as a result of their unlawful acts, omissions, and practices.

F. For an Order granted the declaratory and injunctive relief sought herein.

G. For an award to Plaintiff the costs and disbursements of the action,

H. For an award pre-and post-judgment interest at the maximum legal rate.

I. For any such relief the Court may deem appropriate.

JURY TRIAL DEMANDED

Plaintiff demands a trial by jury on all claims so triable.

Dated: March 12, 2024

Respectfully submitted,

By: /s/E. Michelle Drake

E. Michelle Drake, Bar No. 0387366
BERGER MONTAGUE PC
1229 Tyler Street NE, Suite 205
Minneapolis, MN 55413

Telephone: (612) 594-5933
emdrake@bm.net

Sabita J. Soneji (application for *pro hac vice* admission forthcoming)
TYCKO & ZAVAREEI LLP
1970 Broadway, Suite 1070
Oakland, California 94612
Telephone: (510) 254-6808
ssoneji@tzlegal.com

Counsel for Plaintiff and the Proposed Class